Claims

[c1] 1.Method for normalization of traffic data that is simultaneously transferred to a network intrusion detection system (NIDS) and a monitored end-system located in a network in which packets of data are fragmented and reassembled, characterised in that the method comprises dynamically establishing and maintaining a normalisation table into which information of received fragments and/or the topology of the network comprising the network intrusion detection system (NIDS) and the monitored end-system are entered and received packets of data are modified, redirected or discarded in the event that ambiguities are detected when comparing information contained in the normalization table with information contained in the headers of the received data packets.

[c2] 2.Method according to claim 1, wherein fragments received are registered in the normalization table and forwarded to the end-system immediately thereafter in the event that no conflict is detected with data of previously received fragments or discarded or redirected in case that a conflict is detected.

[c3] 3.Method according to claim 2, wherein for every incoming fragment, based on the content of the header fields IDENTIFICATION, PROTOCOL, SOURCE IP ADDRESS and DESTINATION IP ADDRESS, an identifier is built that allows
a)to assign the fragment to data stored in the normalization table which belongs to earlier received fragments of an identified datagram d_i and to update the normalization table with header data of the received fragment or,
b)in the event that no fragments of the identified datagram were received earlier, to establish a new entry for the identified datagram and update the normalization table with header data of the received fragment.

[c4] 4.Method according to claim 3, wherein for each datagram the header field FRAGMENT OFFSET is extracted and the length of the fragment data is calculated by means of the fields HEADER LENGTH and TOTAL LENGTH in order to establish the structure or information about the received section of the identified datagram without storing data of the identified datagram in said structure or normalization table.

[c5] 5.Method according to claim 3, wherein a partial and complete receipt of an

identified datagram is recorded by means of a sliding bit-mask which is moved to an offset Θ_i depending on the receipt of fragments, belonging to the identified datagram di, until the offset Θ_i indicates receipt of all data contained in the datagram data area of datagram d_i.

[c6] 6.Method according to claim 5, wherein an incoming fragment f with the offset f Θ and the length fv, by means of the sliding bit-mask covering a section of the expected datagram d_i with its length Δ, is

a)discarded in the event that $\Theta_i > f_\Theta$ for the sliding bit-mask going in order or $\Theta_i + \Delta < f_\Theta + fv$ for the sliding bit-mask going in reverse order

a)redirected to a processing unit with a sliding bit-mask of increased length $\Delta_2, \Delta_3, \ldots$ in case that

$\Theta_i + \Delta < f_\Theta +$ fvfor the sliding bit-mask going in order or

$\Theta_i > f_\Theta$ for the sliding bit-mask going in reverse order.

[c7] 7.Method according to claim 2, wherein the registered data belonging to an identified datagram d_i are cleared after the receipt of a corresponding ICMP-message TIMEOUT EXCEEDED WHILE REASSEMBLY or after a time period T1 which is selected equal or slightly higher than the lifetime of the last fragment received and accepted.

[c8] 8.Method according to claim 1, wherein the distance and/or the path MTU to the end-systems in the network that are monitored by the network intrusion detection system (NIDS) are measured and stored in the normalization table before or upon the receipt of a data packet addressed to one of the monitored end-systems.

[c9] 9.Method according to claim 8, wherein for a data packet, such as a datagram or fragment received, the TIME TO LIVE value and/or the path MTU measured for the addressed end-system are retrieved from the normalization table, and

a)in the event that the content in the TIME TO LIVE field is lower than the required value, then it is replaced by the retrieved value and/or

b)in the event that the path MTU is lower than the size of the data packet the do not fragment FLAG, in case that it is set, is cleared.

[c10] 10.Method according to claim 8, wherein the checksum is recalculated for all modified data packets which are forwarded to the addressed end-system.

[c11] 11.Method according to claim 8, wherein the distance and/or the path MTU to an end-system is measured by forwarding a UDP packet with the do not fragment flag DF set and a size corresponding to the maximum transfer unit MTU of the first link towards the addressed end-system, waiting for the return of an ICMP-message and
a)in the event that an ICMP-message FRAGMENTATION REQUIRED BUT DF BIT SET is returned, sending a further UDP packet with reduced size to the addressed end-system and
b)in the event that an ICMP-message PORT NOT REACHABLE is returned, computing the distance to the end-system and storing a required content for the TIME TO LIVE field as well as the probed path MTU in the normalization table.

[c12] 12.Method according to claim 8, wherein an aging bit is added to all entries in the normalization table which is set whenever said entry is retrieved from the normalization table while, periodically after a time period T2, the aging bits of all entries are sequentially reset and entries with aging bits that are already reset are deleted.

[c13] 13.Method according to claim 8, wherein, periodically after a time period T3, the distance and/or the path MTU to the end-systems corresponding to the entries stored in the normalization table are sequentially probed and, in case that values have changed, the normalisation table is updated accordingly.

[c14] 14.Apparatus for normalization of traffic data that is simultaneously transferred to a network intrusion detection system (NIDS) and a monitored end-system located in a network, such as a TCP/IP network, in which packets of data such as IP datagrams, are fragmented and reassembled, the apparatus comprising a stored normalization table that is dynamically established and maintained and into which information of received fragments and/or the topology of the network comprising the network intrusion detection system (NIDS) and the monitored end-system are entered and packets of data such as IP datagrams

are modified, redirected or discarded in case that ambiguities are detected when comparing information contained in the normalization table with information contained in the headers of the received data packets.

[c15] 15.Apparatus according to claim 14 with a control point connected to a network processor which receives the traffic to be normalized by means of the normalization table.

[c16] 16.Apparatus according to claim 15, wherein control programs for probing and periodically updating characteristic values of the network topology are stored in the control point while programs for monitoring receipt of fragments, normalizing data, such as adjusting the content of the TIME TO LIVE field or resetting the do not fragment flag DF whenever required, and/or eliminating over aged entries in the normalization table are stored in the network processor.

[c17] 17.A computer program element comprising computer program code means which, when loaded in a processor of a data processing system, configures the processor to perform a method as claimed in claim 1.